JOURNAL OF COMBINATORIAL THEORY (A) 12, 390–395 (1972)

An Infinite Class of 5-Designs

W. O. ALLTOP

Michelson Laboratories, China Lake, California 93555

Communicated by Marshall Hall, Jr.

Received December 1, 1969

$(\Omega, \mathscr{D})$ is called a t-(v, k, λ) design provided $|\Omega| = v$ and $\mathscr{D}$ is a family of k-subsets of Ω such that every t-subset of Ω is contained in exactly λ members of $\mathscr{D}$. Here we construct a 5-$(2^n + 2, 2^{n-1} + 1, \lambda)$ design for every $n \geqslant 4$, with $\lambda = (2^{n-1} - 3)(2^{n-2} - 1)$. Letting Ω be the projective line over GF(2^n), we first construct a 4-$(2^n + 1, 2^{n-1}, \lambda)$ design on Ω. Such a design can always be extended to a 5-design.

1. INTRODUCTION

The Mathieu groups M_{12} and M_{24} yield 5-designs on 12 and 24 varieties, respectively. Other 5-designs on 12 and 24 varieties have been discovered (see [3], [7], and [8]). Also in [3] 5-designs on 48 varieties are presented, and 5-designs on 30 varieties are mentioned. In [8] 5-designs on 36, 48 and 60 varieties are also presented. Here we shall construct a 5-design on $2^n + 2$ varieties for every $n \geqslant 4$.

If G is a non-trivial t-ply transitive group acting on a set Ω of v varieties and $\mathscr{D}$ is an orbit of k-subsets of Ω, $k > t$, then $(\Omega, \mathscr{D})$ is a t-(v, k, λ) design. The design is trivial only if G is k-homogeneous. The results of [4] guarantee that G is not k-homogeneous for every $k \leqslant v$ whenever $v \geqslant 10$. Therefore, a t-ply transitive group usually yields many non-trivial t-designs.

The triply transitive projective group PGL$(2, q)$ yields non-trivial 3-designs on $q + 1$ varieties for q a prime power $= 7$ or $\geqslant 9$. The affine group AF$(n, 2)$ of n-dimensional affine space over GF(2) yields 3-designs on 2^n varieties for $n \geqslant 3$. Thus, infinitely many 3-designs are obtainable via well-known triply transitive groups. In addition, the existence of a 3-$(v, 4, \lambda)$ design, v and λ satisfying basic necessary conditions, is demonstrated in [5] and [6]. The author has constructed a less interesting, although infinite, class of 3-designs (see [2]), less interesting in that all of the λ's are very large. These and other known classes of 3-designs give one access to an abundance of 3-designs. On the other hand, the Mathieu groups M_{11}, M_{23} and M_{12}, M_{24} remain the only known non-trivial quadruply and quintuply transitive groups, respectively. Nonetheless, infinitely many 4-designs are known (see [1]).

In Section 2, we shall give some essential properties of two of the 3-designs obtained from orbits under the affine group AF(n, 2). In Section 3, the 4-$(2^n + 1, 2^{n-1}, \lambda)$ designs will be constructed, and, in Section 4, the extension theorem will be proved. We shall always denote the family of k-subsets of a set S by $\sum_k(S)$.

2. The 3-Designs in Affine Space

Let E be an n-dimensional vector space over GF(2), $n \geqslant 4$, and let L denote the linear group GL(n, 2) acting doubly transitively on $E - \{0\}$. Now let H be the group of translations $T_\alpha : \omega \to \omega + \alpha$, $\alpha \in E$. The affine group $\mathrm{AF}(n, 2) = \langle L, H \rangle$ is triply transitive on E. Moreover, AF(n, 2) decomposes $\sum_4(E)$ into only two orbits $\mathscr{S}_0$ and $\mathscr{S}_1$, where

$$\mathscr{S}_0 = \{\{\omega_1, \omega_2, \omega_3, \omega_4\} : \textstyle\sum \omega_i = 0\},$$
$$\mathscr{S}_1 = \textstyle\sum_4(E) - \mathscr{S}_0 .$$

$(E, \mathscr{S}_0)$ is a 3-$(2^n, 4, 1)$ design, so we have

$$|\mathscr{S}_0| = \frac{1}{4}\binom{2^n}{3},$$
$$|\mathscr{S}_1| = (2^{n-2} - 1)\binom{2^n}{3}.$$

Let Δ be an $(n - 1)$-dimensional subspace of E and let $\mathscr{E}$ be the orbit of Δ under AF(n, 2). Since $\mathscr{E}$ consists of the $2^n - 1$ subspaces of E of dimension $n - 1$ and their cosets, we have $|\mathscr{E}| = 2^{n+1} - 2$. Therefore, $(E, \mathscr{E})$ is a 3-$(2^n, 2^{n-1}, 2^{n-2} - 1)$ design. Since $\mathscr{S}_0$ and $\mathscr{E}$ are orbits under AF(n, 2), each member of $\mathscr{S}_0$ is contained in the same number of members of $\mathscr{E}$. Since each member of $\mathscr{E}$ contains $\frac{1}{4}\binom{2^{n-1}}{3}$ members of $\mathscr{S}_0$, it follows that each member of $\mathscr{S}_0$ is contained in $2^{n-2} - 1$ members of $\mathscr{E}$. It also follows that each member of $\mathscr{S}_1$ is contained in $2^{n-3} - 1$ members of $\mathscr{E}$. This information will be helpful in Section 3 inasmuch as our 4-designs decompose into disjoint 3-designs isomorphic to $(E, \mathscr{E})$.

3. The 4-Designs

Let $E = \mathrm{GF}(2^n)$, $n \geqslant 4$, $\Omega = E \cup \{\infty\}$, and $E^* = E - \{0\}$. Let G denote the group of linear fractional transformations $\omega \to (\alpha\omega + \beta)/(\gamma\omega + \delta)$

acting triply transitively on Ω. Let G_∞ be the stabilizer of ∞ in G. As in Section 2, we let Δ be an $(n-1)$-dimensional subspace of E, considering E only as a vector space over GF(2). Now let $\mathscr{D}$ be the orbit of Δ under the action of G. Our goal in this section is to show that $(\Omega, \mathscr{D})$ is a 4-design with $\lambda = (2^{n-1}-3)(2^{n-2}-1)$.

First let $\mathscr{D}_\infty$ denote the orbit of Δ under G_∞. Let $M = \langle x \rangle$ where x is defined by $\omega x = \gamma\omega$, γ a primitive root of E. Let D be the stabilizer of Δ in G, $D_\infty = D \cap G_\infty$ and $D^* = D \cap M$. For some integers r, s, we have $D^* = \langle x^r \rangle$ where $rs = 2^n - 1$. Now D^* decomposes $\Delta - \{0\}$ into orbits of size s. Therefore, $s \mid (2^{n-1}-1)$ and $s \mid (2^n - 1)$. It follows that $s = 1$ and $D^* = \langle 1 \rangle$.

M acts regularly on the family of $2^n - 1$ subspaces of dimension $n-1$ in E. We see that $\mathscr{D}_\infty$ is the same family of subspaces and their cosets as the family $\mathscr{E}$ of Section 2, so $(E, \mathscr{D}_\infty)$ is a 3-design isomorphic to $(E, \mathscr{E})$. Moreover, D_∞ must be the group of translations $\omega \to \omega + \delta$, $\delta \in \Delta$.

Now suppose D_∞ is properly contained in D. There exists $y \in D$ such that $\infty y \neq \infty$. Since D_∞ is transitive on $E - \Delta$, D must be transitive on $\Omega - \Delta$. But $|\Omega - \Delta| = 2^{n-1} + 1$. Since $2^{n-1}+1$ divides $|D|$, $2^{n-1}+1$ must also divide $|G|$. But $2^{n-1}+1$ divides $|G|$ only when $n \leqslant 2$. We conclude that $D = D_\infty$.

The stabilizer of Δ admits the unique fixed point ∞. Likewise, for every Γ in $\mathscr{D}$, the stabilizer of Γ fixes a unique point. For $\omega \in \Omega$, let $\mathscr{D}_\omega$ denote the subfamily of $\mathscr{D}$ consisting of those blocks whose stabilizers fix ω. We have a decomposition

$$\mathscr{D} = \bigcup \{\mathscr{D}_\omega : \omega \in \Omega\}$$

of $\mathscr{D}$ into disjoint families, where every design $(\Omega - \{\omega\}, \mathscr{D}_\omega)$ is a 3-$(2^n, 2^{n-1}, 2^{n-2}-1)$ design isomorphic to $(E, \mathscr{E})$. For each ω in Ω, the family $\mathscr{D}_\omega$ uniquely determines a decomposition of $\sum_4(\Omega - \{\omega\})$ into two subfamilies $\mathscr{S}_0^\omega$, $\mathscr{S}_1^\omega$ satisfying the following: each member of $\mathscr{S}_0^\omega$ is contained in $2^{n-2}-1$ members of $\mathscr{D}_\omega$, each member of $\mathscr{S}_1^\omega$ is contained in $2^{n-3}-1$ members of $\mathscr{D}_\omega$. Now suppose Q is any member of $\sum_4(\Omega)$. Since G is triply transitive on Ω there exist $u \in G$ and $\alpha \in E^\# - \{1\}$ such that $Qu = \{\infty, 0, 1, \alpha\}$. Now define v by

$$v\colon \omega \to (\alpha + \sqrt{\alpha})/(\omega + \sqrt{\alpha}).$$

We have

$$Quv = \{0, 1 + \sqrt{\alpha}, \sqrt{\alpha}, 1\} \in \mathscr{S}_0^\infty.$$

Thus, $Q \in \mathscr{S}_0^\omega$ where $\omega = \infty\, v^{-1} u^{-1}$. Every member of $\sum_4(\Omega)$ is an element of $\mathscr{S}_0^\omega$ for some ω. Since there are $2^n + 1$ families $\mathscr{D}_\omega$, and for each ω we have

$$| \mathscr{S}_0^\omega | = \frac{1}{4}\binom{2^n}{3},$$

it follows that there are $\binom{2^n+1}{4}$ pairs (Q, ω) such that $Q \in \mathscr{S}_0^\omega$. From this we see that every quadruple Q is an element of $\mathscr{S}_0^\omega$ for exactly one ω. (It is not difficult to show that $Q \in \mathscr{S}_0^\omega$, where ω is the unique fixed point of the stabilizer of Q in G.) Therefore, Q is in $2^{n-2} - 1$ members of $\mathscr{D}_\omega$ and $2^{n-3} - 1$ members of $\mathscr{D}_\sigma$ for $\sigma \in \Omega - (Q \cup \{\omega\})$. It follows that Q is contained in $(2^{n-1} - 3)(2^{n-2} - 1)$ members of $\mathscr{D}$ independent of the quadruple Q. Therefore, $(\Omega, \mathscr{D})$ is the desired 4-design.

4. Extending t-Designs

Suppose $(\Omega, \mathscr{D})$ is a $t - (2k + 1, k, \lambda)$ design. Let $\Omega^- = \Omega \cup \{X\}$, $X \notin \Omega$, and let $\mathscr{D}^- = \mathscr{D}' \cup \mathscr{D}''$ where

$$\mathscr{D}' = \{\{X\} \cup \Delta : \Delta \in \mathscr{D}\},$$
$$\mathscr{D}'' = \{\Omega - \Delta : \Delta \in \mathscr{D}\}.$$

Our goal in this section is to prove the following

Extension Theorem. *If t is even, then $(\Omega^-, \mathscr{D}^-)$ is a*

$$(t + 1) - (2k + 2, k + 1, \lambda)$$

design.

Proof. Since $(\Omega, \mathscr{D})$ is a j-design, $0 \leqslant j \leqslant t$, we may let λ_j denote the number of blocks of $\mathscr{D}$ containing a fixed j-subset of Ω. Suppose T is a $(t + 1)$-subset of Ω^-. If $X \in T$, then T is contained in λ members of $\mathscr{D}'$ and no members of $\mathscr{D}''$.

On the other hand, suppose X is not in T. Let λ^- be the number of blocks in $\mathscr{D}^-$ containing T. We have $\lambda^- = \zeta + \xi$ where ζ is the number of blocks in $\mathscr{D}$ containing T, ξ the number of blocks in $\mathscr{D}$ disjoint from T. For a fixed s-subset S of T, let η_s be the number of blocks $\Gamma \in \mathscr{D}$ such that $T \cap \Gamma = S$. Perhaps it is not obvious that η_s is independent of the choice of S in T. We shall prove this independence. Clearly $\eta_{t+1} = \zeta$. Now suppose S is a t-subset of T. Of the λ_t blocks in $\mathscr{D}$ containing S exactly ζ of them contain T. Hence, $\eta_t = \lambda_t - \zeta$, independent of S. We proceed by induction. Our induction hypothesis $H(m)$ will be the following:

$$\eta_{t-i+1} = \Lambda_{t-i+1} + (-1)^i\zeta \qquad \text{for} \quad 0 \leqslant i \leqslant m,$$

where Λ_{t-i+1} is a linear combination of λ_t, $\lambda_{t-1}, \ldots, \lambda_{t-i+1}$ which is independent of T as well as S. We have proved $H(1)$. Assuming $H(m-1)$, $2 \leqslant m \leqslant t+1$, suppose S is a $(t-m+1)$-subset of T. For

$$1 \leqslant i \leqslant m-1$$

there are $\binom{m}{i}$ subsets U of T such that $|U| = t-m+i+1$ and $S \subset U \subset T$. For each such U there are $\eta_{t-m+i+1}$ blocks Γ in $\mathscr{D}$ such that $T \cap \Gamma = U$. Therefore, the number of blocks in $\mathscr{D}$ which meet T in S is η_{t-m+1}, where

$$\begin{aligned}\eta_{t-m+1} &= \lambda_{t-m+1} - \sum_{i=1}^{m-1} \binom{m}{i} \eta_{t-m+i+1} - \zeta \\ &= \Lambda_{t-m+1} + (-1)^m \zeta;\end{aligned}$$

and

$$\Lambda_{t-m+1} = \lambda_{t-m+1} - \sum_{i=1}^{m-1} \binom{m}{i} \Lambda_{t-m+i+1}.$$

This completes the induction. More specifically it can be shown that

$$\Lambda_{t-m+1} = \sum_{i=0}^{m-1} (-1)^i \binom{m}{i} \lambda_{t-m+i+1}.$$

We now have $\xi = \eta_0 = \Lambda_0 + (-1)^{t+1}\zeta$. If t is even, then $\zeta + \xi = \Lambda_0$. Therefore, for t even, λ^- is independent of T.

Now let ρ be the number of pairs (T, Δ^-) such that $T \in \sum_{t+1}(\Omega^-)$, $\Delta^- \in \mathscr{D}^-$ and $T \subset \Delta^-$. We have shown that $\lambda\binom{2k+1}{t}$ pairs have first coordinate containing X, while $\lambda^-\binom{2k+1}{t+1}$ pairs have first coordinate not containing X. Hence,

$$\rho = \lambda \binom{2k+1}{t} + \lambda^- \binom{2k+1}{t+1}.$$

On the other hand $|\mathscr{D}^-| = 2\lambda_0$, and

$$\lambda_0 = [\lambda(2k+1)!\,(k-t)!]/[k!\,(2k-t+1)!].$$

Each member of $\mathscr{D}^-$ appears as second coordinate of $\binom{k+1}{t+1}$ of the pairs being counted, so

$$\rho = 2\lambda_0 \binom{k+1}{t+1} = \lambda \binom{2k+2}{t+1}.$$

From the equation

$$\lambda\binom{2k+1}{t}+\lambda^-\binom{2k+1}{t+1}=\lambda\binom{2k+2}{t+1}$$

it follows that $\lambda = \lambda^-$. Thus, $(\Omega^-, \mathscr{D}^-)$ is in fact a $(t + 1)$-design.

By adjoining a new variety X to the projective line Ω in this fashion one obtains a 5-$(2^n + 2, 2^{n-1} + 1, \lambda)$ design $(\Omega^-, \mathscr{D}^-)$ from the 4-design of Section 3, with $\lambda = (2^{n-1} - 3)(2^{n-2} - 1)$.

References

1. W. O. Alltop, An infinite class of 4-designs, *J. Combinatorial Theory* **6** (1969), 320–322.
2. W. O. Alltop, Some 3-designs and a 4-design, *J. Combinatorial Theory* (*A*) **11** (1971), 190–195.
3. E. F. Assmus, Jr., and H. F. Mattson, Jr., New 5-designs, *J. Combinatorial Theory* **6** (1969), 122–151.
4. R. A. Beaumont and R. P. Peterson, Set-transitive permutation groups, *Canad. J. Math.* **7** (1955), 35–42.
5. H. Hanani, On quadruple systems, *Canad. J. Math.* **12** (1960), 145–157.
6. H. Hanani, On some tactical configurations, *Canad. J. Math.* **15** (1963), 702–722.
7. D. R. Hughes, *t*-Designs and groups, *Amer. J. Math.* **87** (1965), 761–778.
8. Vera Pless, Symmetry codes over GF(3) and new five-designs, *J. Combinatorial Theory (A)* **12** (1972), 119–142.